210-250.90q

Number: 210-250
Passing Score: 800
Time Limit: 120 min
File Version: 1

Cisco 210-250

Understanding Cisco Cybersecurity Fundamentals

Exam A

QUESTION 1
Which definition of a fork in Linux is true?

A. daemon to execute scheduled commands
B. parentdirectory name of a file path name
C. macros for manipulating CPU sets
D. new process created by a parent process

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Which identifier is used to describe the application or process that submitted a log message?

A. action
B. selector
C. priority
D. facility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://www.tutorialspoint.com/unix/unix-system-logging.htm

QUESTION 3
Which protocol is expected to have a user agent, host, and referrer header in a packet capture?

A. NTP
B. HTTP
C. DNS
D. SSH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation
B. tunneling
C. timing attack
D. resource exhaustion

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:https://books.google.com/books?id=KIwLSddtAWsC&pg=PA58&lpg=PA58&dq=timing+attack
+performing+actions+slower+than+normal+to+prevent+detection&source=bl&ots=9qu7ywV-
mX&sig=_9lwcDDq-
WNaYlEeP7VkR0MPAOE&hl=en&sa=X&ved=0ahUKEwiRwo_P8vvRAhVKyoMKHaUlAUQQ6AEIITAB#v=onep
age&q=timing%20attack%20performing%20actions%20slower%20than%20normal%20to%20prevent%
20detection&f=false

QUESTION 5
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. replay
B. man-in-the-middle
C. dictionary
D. known-plaintext

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Which definition of permissions in Linux is true?

A. rules that allow network traffic to go in and out
B. table maintenance program
C. written affidavit that you have to sign before using the system
D. attributes of ownership and control of an object

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Which definition describes the main purpose of a Security Information and Event Management solution?

A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats
B. a monitoring interface that manages firewall access control lists for duplicate firewall filtering
C. a relay server or device that collects then forwards event logs to another log collection device
D. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture of an environment

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 8
If a web server accepts input from the user and passes it to a bash shell, to which attack method if it vulnerable?

A. input validation
B. hash collision
C. command injection
D. integer overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Which security monitoring data type is associated with application server logs?

A. alert data
B. statistical data
C. session data
D. transaction data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Which two terms are types of cross site scripting attacks? (Choose two.)

A. directed
B. encoded
C. stored
D. reflected
E. cascaded

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Which two actions are valid uses of public key infrastructure? (Choose two.)

A. ensuring the privacy of a certificate
B. revoking the validation of a certificate
C. validating the authenticity of a certificate
D. creating duplicate copies of a certificate
E. changing ownership of a certificate

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
Which definition of a process in Windows is true?

A. running program
B. unit of execution that must be manually scheduled by the application
C. database that stores low-level settings for the OS and for certain applications
D. basic unit to which the operating system allocates processor time

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
Which tool is commonly used by threat actors on a webpage to take advantage of the software vulnerabilities of a system to spread malware?

A. exploit kit
B. root kit
C. vulnerability kit
D. script kiddie kit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
Which encryption algorithm is the strongest?

A. AES
B. CES
C. DES
D. 3DES

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully?

A. ACK
B. SYN, ACK
C. RST
D. PSH, ACK

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Which two tasks can be performed by analyzing the logs of a traditional stateful firewall? (Choose two.)

A. Confirm the timing of network connections differentiated by the TCP 5-tuple.
B. Audit the applications used within a social networking web site.
C. Determine the user IDs involved in an instant messaging exchange.
D. Map internal private IP addresses to dynamically translated external public IP addresses.
E. Identify the malware variant carried by an SMTP connection

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
Which term represents a potential danger that could take advantage of a weakness in a system?

A. vulnerability
B. risk
C. threat
D. exploit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

A. traffic fragmentation
B. resource exhaustion
C. timing attack
D. tunneling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which term represents the chronological record of how evidence was collected, analyzed, preserved, and transferred?

A. chain of evidence
B. evidence chronology
C. chain of custody
D. record of safekeeping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
In computer security, which information is the term PHI used to describe?

A. private host information
B. protected health information
C. personal health information
D. protected host information

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
For which reason can HTTPS traffic make security monitoring difficult?

A. encryption
B. large packet headers
C. Signature detection takes longer
D. SSL interception

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which network device is used to separate broadcast domains?

A. router
B. repeater
C. switch
D. bridge

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Which term describes the act of a user, without authority or permission, obtaining rights on a system, beyond what were assigned?

A. authentication tunneling
B. administrative abuse
C. rights exploitation
D. privilege escalation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. integrity validation
B. due diligence
C. need to know
D. least privilege

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Based on which statement does the discretionary access control security model grant or restrict access?

A. discretion of the system administrator
B. security policy defined by the owner of an object

C. security policy defined by the system administrator
D. role of a user within an organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which event occurs when a signature-based IDS encounters network traffic that triggers an alert?

A. connection event
B. endpoint event
C. NetFlow event
D. intrusion event

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
One of the objectives of information security if to protect the CIA of information and systems. What does CIA mean in this context?

A. Confidentiality, Integrity, and Availability
B. Confidentiality, Identity, and Availability
C. Confidentiality, Integrity, and Authorization
D. Confidentiality, Identity, and Authorization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

A. HTTP/TLS
B. IPv4/IPv6
C. TCP/UDP
D. ATM/MPLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Which information security property is supported by encryption?

A. sustainability
B. integrity
C. confidentiality
D. availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which two activities are examples of social engineering? (Choose two.)

A. receiving call from the IT department asking you to verify your username/password to maintain the account
B. receiving an invite to your department's weekly WebEx meeting
C. sending a verbal request to an administrator to change the password to the account of a user the administrator does know
D. receiving an email from HR requesting that you visit the secure HR website and update your contract information
E. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company

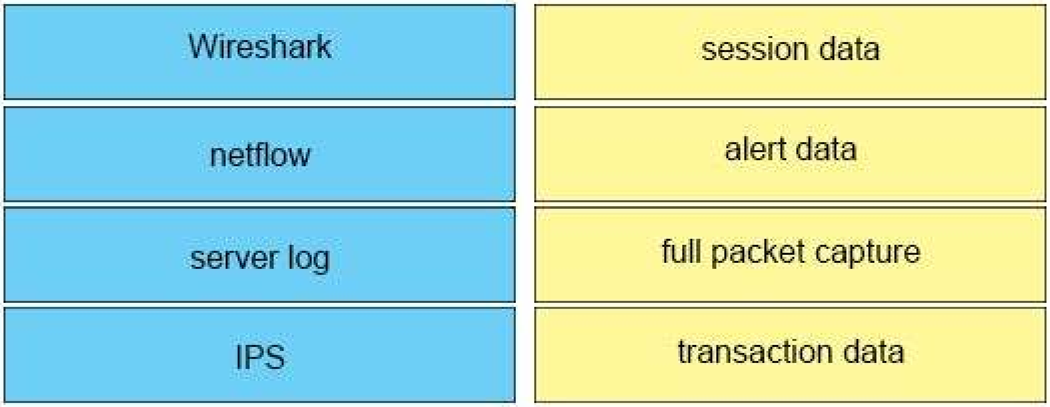
Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
DRAG DROP

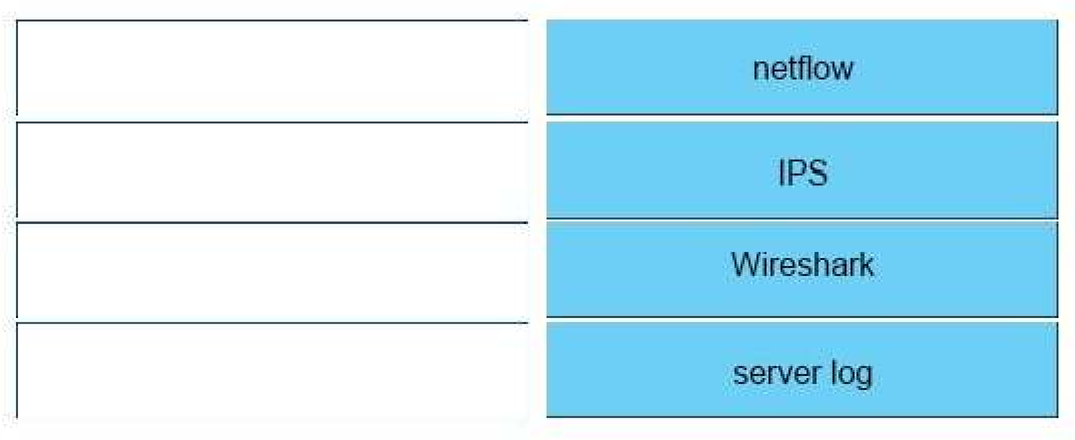
Drag the data source on the left to the correct data type on the right.

Select and Place:



Wireshark	session data
netflow	alert data
server log	full packet capture
IPS	transaction data

Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which protocol maps IP network addresses to MAC hardware addresses so that IP packets can be sent across networks?

A. Internet Control Message Protocol
B. Address Resolution Protocol
C. Session Initiation Protocol
D. Transmission Control Protocol/Internet Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
Which option is an advantage to using network-based anti-virus versus host-based anti-virus?

A. Network-based has the ability to protect unmanaged devices and unsupported operating systems.
B. There are no advantages compared to host-based antivirus.
C. Host-based antivirus does not have the ability to collect newly created signatures.
D. Network-based can protect against infection from malicious files at rest.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
Which concern is important when monitoring NTP servers for abnormal levels of traffic?

A. Being the cause of a distributed reflection denial of service attack.
B. Users changing the time settings on their systems.
C. A critical server may not have the correct time synchronized.
D. Watching for rogue devices that have been added to the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
While viewing packet capture data, you notice that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which option is making this behavior possible?

A. TOR
B. NAT
C. encapsulation
D. tunneling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
Which hashing algorithm is the least secure?

A. MD5
B. RC4
C. SHA-3
D. SHA-2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
You must create a vulnerability management framework. Which main purpose of this framework is true?

A. Conduct vulnerability scans on the network.
B. Manage a list of reported vulnerabilities.
C. Identify, remove, and mitigate system vulnerabilities.
D. Detect and remove vulnerabilities in source code.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
Which definition of Windows Registry is true?

A. set of pages that are currently resident in physical memory
B. basic unit to which the operating system allocates processor time
C. set of virtual memory addresses
D. database that stores low-level settings for the operating system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
Which two features must a next generation firewall include? (Choose two.)

A. data mining
B. host-based antivirus
C. application visibility and control
D. Security Information and Event Management
E. intrusion detection system

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Which type of exploit normally requires the culprit to have prior access to the target system?

A. local exploit
B. denial of service
C. system vulnerability
D. remote exploit

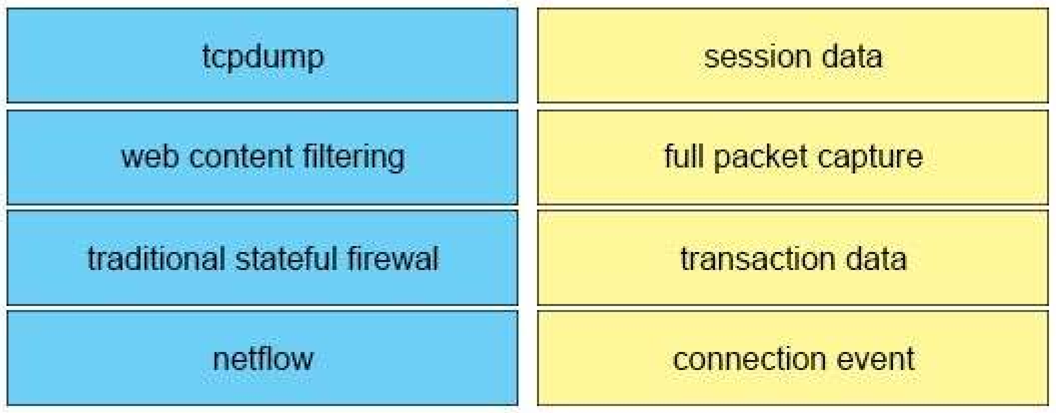
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
DRAG DROP

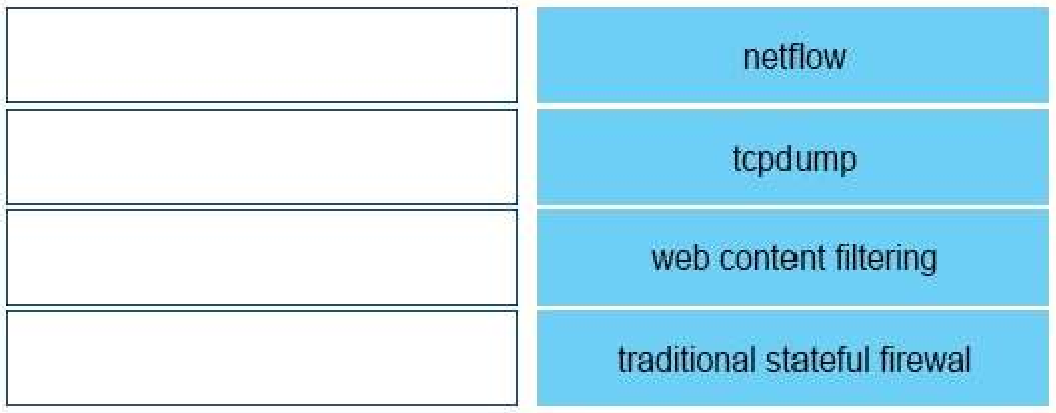
Drag the technology on the left to the data type the technology provides on the right.

Select and Place:



tcpdump	session data
web content filtering	full packet capture
traditional stateful firewal	transaction data
netflow	connection event

Correct Answer:



	netflow
	tcpdump
	web content filtering
	traditional stateful firewal

Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which two options are recognized forms of phishing? (Choose two.)

A. spear
B. whaling
C. mailbomb
D. hooking
E. mailnet

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
According to RFC 1035, which transport protocol is recommended for use with DNS queries?

A. Transmission Control Protocol
B. Reliable Data Protocol
C. Hypertext Transfer Protocol
D. User Datagram Protocol

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
Which statement about digitally signing a document is true?

A. The document is hashed and then thedocument is encrypted with the private key.
B. The document is hashed and then the hash is encrypted with the private key.
C. The document is encrypted and then the document is hashed with the public key.
D. The document is hashed and then the document isencrypted with the public key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
Which term represents a weakness in a system that could lead to the system being compromised?

A. vulnerability
B. threat
C. exploit
D. risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
Which security principle states that more than one person is required to perform a critical task?

A. due diligence
B. separation of duties
C. need to know
D. least privilege

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
Which definition of a daemon on Linux is true?

A. error check right afterthe call to fork a process
B. new process created by duplicating the calling process
C. program that runs unobtrusively in the background
D. set of basic CPU instructions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
Which directory is commonly used on Linux systems to store log files, including syslog and apache access logs?

A. /etc/log
B. /root/log
C. /lib/log
D. /var/log

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
A user reports difficulties accessing certain external web pages. When examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

A. insufficient network resources
B. failure offull packet capture solution
C. misconfiguration of web filter
D. TCP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
Which security monitoring data type requires the most storage space?

A. full packet capture

B. transaction data
C. statistical data
D. session data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
Which hash algorithm is the weakest?

A. SHA-512
B. RSA 4096
C. SHA-1
D. SHA-256

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
Where is a host-based intrusion detection system located?

A. on a particular end-point as an agent or a desktop application
B. on a dedicated proxy server monitoring egress traffic
C. on a span switch port
D. on a tap switch port

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
Which definition of the IIS Log Parser tool is true?

A. a logging module for IIS that allows you to logto a database
B. a data source control to connect to your data source
C. a powerful, versatile tool that makes it possible to run SQL-like queries against log files
D. a powerful, versatile tool that verifies the integrity of the log files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
A firewall requires deep packet inspection to evaluate which layer?

A. application
B. internet
C. link
D. transport

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
Which definition of vulnerability is true?

A. an exploitable, unpatched and unmitigated weakness in software
B. an incompatible piece of software
C. software that does not have the most current patch applied
D. software that was not approved for installation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
Which cryptographic key is contained in an X.509 certificate?

A. symmetric
B. public
C. private
D. asymmetric

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which option is a purpose of port scanning?

A. Identify the Internet Protocol of the target system.
B. Determine if the network is up or down.
C. Identify which ports and services are open on the target host.
D. Identify legitimate users of a system.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Which two protocols are used for email? (Choose two.)

A. NTP
B. DNS
C. HTTP
D. IMAP
E. SMTP

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

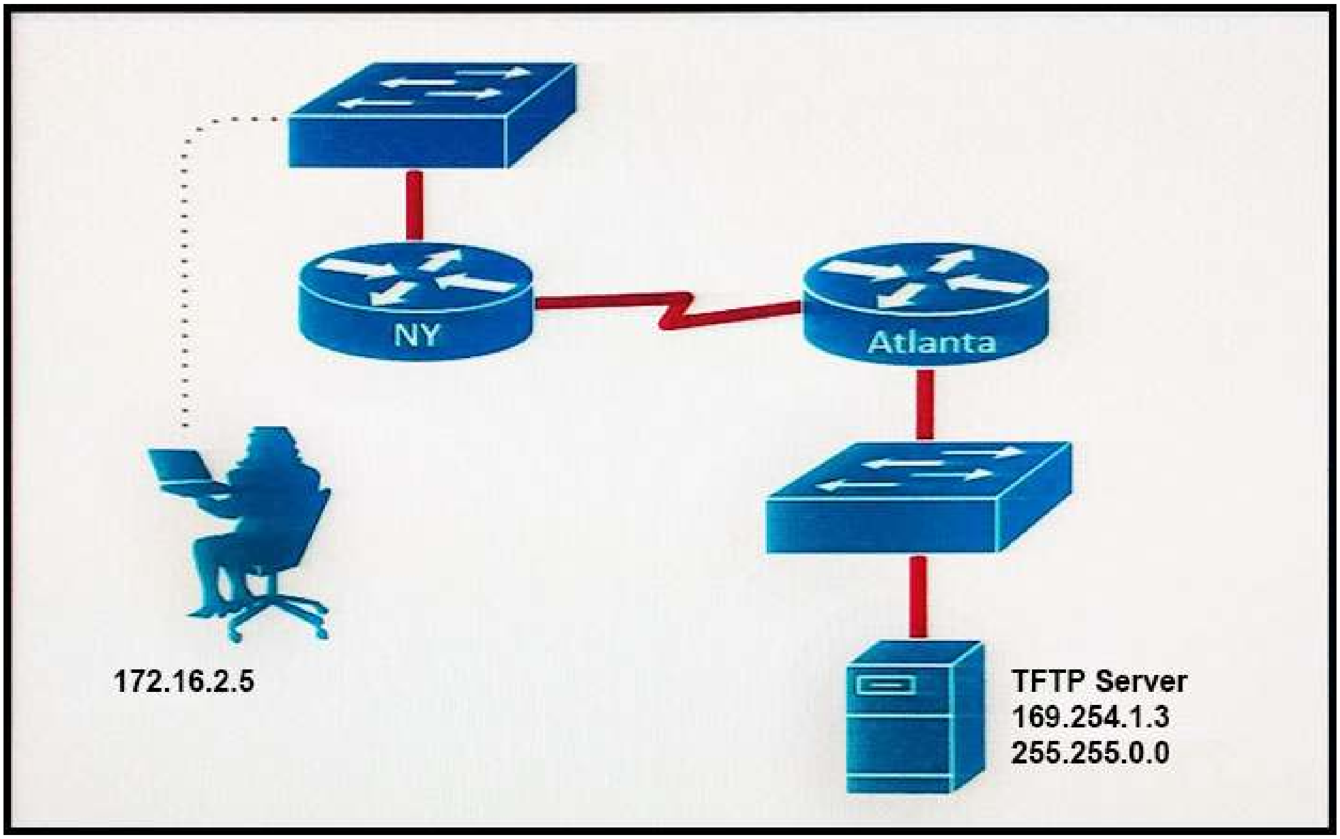
QUESTION 59
Which definition of the virtual address space for a Windows process is true?

A. actual physical location of an object in memory
B. set of virtual memory addresses that it can use
C. set of pages that are currently resident in physical memory
D. system-level memory protection feature that is built into the operating system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60



Refer to the exhibit. A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to backup the configuration file and Cisco IOS of the NY router to the TFTP server. Which cause of this problem is true?

A. The TFTP server cannot obtain an address from a DHCP Server
B. The TFTP server has an incorrect IP address.
C. The network administrator computer has an incorrect IP address.
D. The TFTP server has an incorrect subnet mask.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Which data can be obtained using NetFlow?

A. session data
B. applicationlogs
C. network downtime report
D. full packet capture

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Which situation indicates application-level whitelisting?

A. Allow everything and deny specific executable files.
B. Allow specific executable files and deny specific executable files.
C. Writing current application attacks on a whiteboard daily.
D. Allow specific files and deny everything else.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

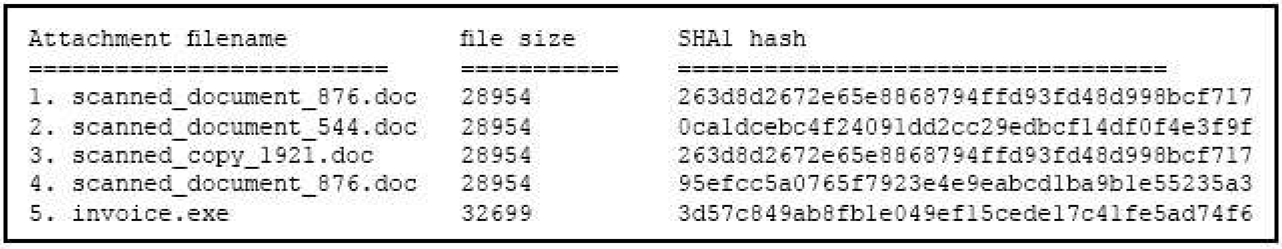
QUESTION 63
Which definition of an antivirus program is true?

A. program used to detect and remove unwanted malicious software from the system
B. program that provides real-time analysis of security alerts generated by network hardware and applications
C. program that scans a running application for vulnerabilities
D. rules that allow network traffic to go in and out

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64



```
Attachment filename            file size      SHA1 hash
=========================      ===========    ==================================
1. scanned_document_876.doc    28954          263d8d2672e65e8868794ffd93fd48d998bcf717
2. scanned_document_544.doc    28954          0ca1dcebc4f24091dd2cc29edbcf14df0f4e3f9f
3. scanned_copy_1921.doc       28954          263d8d2672e65e8868794ffd93fd48d998bcf717
4. scanned_document_876.doc    28954          95efcc5a0765f7923e4e9eabcd1ba9b1e55235a3
5. invoice.exe                 32699          3d57c849ab8fb1e049ef15cede17c41fe5ad74f6
```

Refer to the exhibit. During an analysis, this list of email attachments is found. Which files contain the same content?

A. 1 and 4
B. 3 and 4
C. 1 and 3
D. 1 and 2

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target?

A. main in the middle
B. denial of service
C. distributed denial of service
D. replay

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which technology allows a large number of private IP addresses to be represented by a smaller number of public IP addresses?

A. NAT
B. NTP
C. RFC 1631
D. RFC 1918

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which NTP command configures the local device as an NTP reference clock source?

A. ntp peer
B. ntp broadcast
C. ntp master
D. ntp server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Which three options are types of Layer 2 network attack? (Choose three.)

A. ARP attacks
B. brute force attacks
C. spoofing attacks
D. DDOS attacks
E. VLAN hopping
F. botnet attacks

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

A. 1
B. 2
C. 4
D. 8

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Where does routing occur within the DoD TCP/IP reference model?

A. application
B. internet
C. network
D. transport

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What is PHI?

A. Protected HIPAA information
B. Protected health information
C. Personal health information
D. Personal human information

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following are Cisco cloud security solutions?

A. CloudDLP
B. OpenDNS
C. CloudLock
D. CloudSLS

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
What is a trunk link used for?

A. To pass multiple virtual LANs
B. To connect more than two switches
C. To enable Spanning Tree Protocol
D. To encapsulate Layer 2 frames

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
At which OSI layer does a router typically operate?

A. Transport
B. Network
C. Data link
D. Application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Cisco pxGrid has a unified framework with an open API designed in a hub-and-spoke architecture. pxGrid is used to enable the sharing of contextual-based information from which devices?

A. From a Cisco ASA to the Cisco OpenDNS service

B. From a Cisco ASA to the Cisco WSA

C. From a Cisco ASA to the Cisco FMC

D. From a Cisco ISE session directory to other policy network systems, such as Cisco IOS devices and the Cisco ASA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
What are the advantages of a full-duplex transmission mode compared to half-duplex mode? (Select all that apply.)

A. Each station can transmit and receive at the same time.

B. It avoids collisions.

C. It makes use of backoff time.

D. It uses a collision avoidance algorithm to transmit.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs).
They inspect which of the following elements within a packet? (Choose two.)

A. Session headers

B. NetFlow flow information

C. Source and destination ports and source and destination IP addresses

D. Protocol information

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
In which case should an employee return his laptop to the organization?

A. When moving to a different role

B. Upon termination of the employment

C. As described in the asset return policy

D. When the laptop is end of lease

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 79
Which of the following are metrics that can measure the effectiveness of a runbook?

A. Mean time to repair (MTTR)
B. Mean time between failures (MTBF)
C. Mean time to discover a security incident
D. All of the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following access control models use security labels to make access decisions?

A. Mandatory access control (MAC)
B. Role-based access control (RBAC)
C. Identity-based access control (IBAC)
D. Discretionary access control (DAC)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
MAC uses security labels for access decisions.

QUESTION 81
Where are configuration records stored?

A. In a CMDB
B. In a MySQL DB
C. In a XLS file
D. There is no need to store them

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following is true about heuristic-based algorithms?

A. Heuristic-based algorithms may require fine tuning to adapt to network traffic and minimize the possibility of false positives.

B. Heuristic-based algorithms do not require fine tuning.
C. Heuristic-based algorithms support advanced malware protection.
D. Heuristic-based algorithms provide capabilities for the automation of IPS signature creation and tuning.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
How many broadcast domains are created if three hosts are connected to a Layer 2 switch in full-duplex mode?

A. 4
B. 3
C. None
D. 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
What is one of the advantages of the mandatory access control (MAC) model?

A. Stricter control over the information access.
B. Easy and scalable.
C. The owner can decide whom to grant access to.
D. Complex to administer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Strict control over the access to resources is one of the main advantages of MAC.

QUESTION 85
According to the attribute-based access control (ABAC) model, what is the subject location considered?

A. Part of the environmental attributes
B. Part of the object attributes
C. Part of the access control attributes
D. None of the above

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
What type of algorithm uses the same key to encryp and decrypt data?

A. a symmetric algorithm
B. an asymmetric algorithm
C. a Public Key infrastructure algorithm
D. an IP Security algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which actions can a promiscuous IPS take to mitigate an attack?

A. modifying packets
B. requesting connection blocking
C. denying packets
D. resetting the TCP connection
E. requesting host blocking
F. denying frames

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which Statement about personal firewalls is true?

A. They are resilient against kernal attacks
B. They can protect email messages and private documents in a similar way to a VPN
C. They can protect the network against attacks
D. They can protect a system by denying probing requests

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files
B. It can be deployed at the perimeter
C. It uses signature-based policies

D. It can have more restrictive policies than network-based IPS
E. It works with deployed firewalls
F. It can generate alerts based on behavior at the desktop level.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
An attacker installs a rogue switch that sends superior BPDUs on your network.
What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain
D. The switch could become a transparent bridge.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: